CLAIMS

1. A method for assembling fragmented network traffic, comprising:

detecting in the fragmented network traffic an anomaly that could result in two or more fragments comprising the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than the corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed; and

performing further processing on the fragmented network traffic having the anomaly.

2. A method as recited in claim 1 wherein detecting an anomaly comprises determining that said two or more fragments overlap.

3. A method as recited in claim 2 wherein determining that said two or more fragments overlap comprises reading a header value associated with one of the fragments.

4. A method as recited in claim 3 wherein the header value comprises an offset value.

5. A method as recited in claim 1 wherein detecting an anomaly comprises determining that said two or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments.

6. A method as recited in claim 1 wherein performing further processing comprises determining configuration information associated with said destination node.

7. A method as recited in claim 6 wherein determining configuration information comprises querying the destination node.

8. A method as recited in claim 6 wherein determining configuration information comprises querying an information base.

9. A method as recited in claim 1 wherein performing further processing comprises reassembling the fragmented network traffic to generate more than one variant of the reassembled data flow.

10. A method as recited in claim 1 further including processing the anomaly to determine whether the fragmented network traffic is associated with a threat.

11. A method as recited in claim 1 further including performing an action on the fragmented network traffic based on whether the fragmented network traffic is associated with a threat.

12. A method as recited in claim 1 further including discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat.

13. A method as recited in claim 1 further including copying one or more fragments comprising the fragmented network traffic to a buffer.

14. A method as recited in claim 1 wherein performing further processing comprises sending an alert.

15. A method as recited in claim 1 wherein performing further processing comprises determining whether the fragmented network traffic should be blocked.

16. A method as recited in claim 1 wherein performing further processing comprises determining whether the fragmented network traffic should be forwarded to the destination node.

17. A method as recited in claim 1 wherein performing further processing comprises determining whether to initiate increased buffering of the fragmented network traffic.

18. A method as recited in claim 1 wherein performing further processing comprises initiating increased buffering of the fragmented network traffic if it is determined that two or more fragments comprising said fragmented network traffic have overlapping portions.

19. A method as recited in claim 1 wherein performing further processing comprises initiating increased buffering of the fragmented network traffic if it is determined that two or more fragments comprising said fragmented network traffic have mismatching overlapping portions.

20. A system for assembling fragmented network traffic, comprising:

a memory configured to store at least a portion of the fragmented network traffic; and

a processor configured to detect in the fragmented network traffic an anomaly that could result in two or more fragments comprising the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than the corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed; and perform further processing on the fragmented network traffic having the anomaly.

21. A computer program product for assembling fragmented network traffic, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

detecting in the fragmented network traffic an anomaly that could result in two or more fragments comprising the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than the corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed; and

performing further processing on the fragmented network traffic having the anomaly.